

REMARKS

In the Office Action dated July 16, 2004, claims 1-3, 6-8, 11-15, 18, 19, 21-23, 27, 28, and 30-39 were rejected under 35 U.S.C § 102 over U.S. Patent No. 6,473,798 (Grosser); claims 4, 5, 16, 17, and 20 were rejected under § 103 over Grosser in view of U.S. Patent No. 6,182,226 (Reid); claims 9, 10, 24, 25, and 29 were rejected under § 103 over Grosser in view of U.S. Patent No. 6,636,898 (Ludovici); and claim 26 was rejected under § 103 over Grosser in view of U.S. Patent No. 6,173,411 (Hirst).

Claims 1, 11, 14, 15, 18, 27, and 31 have been cancelled, without prejudice, to render the rejections of those claims moot.

Former claims 32, 34, 36, and 38 have been amended from dependent form to independent form, with the scope of each of these claims remaining *unchanged*. Independent claims 32, 34, 36, and 38 are not anticipated by Grosser, contrary to the assertion made in the Office Action.

Claim 32 recites a method of determining if a link is alive, comprising:

- establishing a secure link between a first node and second node according to a security protocol;
- sending at least one ping message targeting the second node over the security link, the at least one ping message defined outside the security protocol; and
- monitoring for at least one ping reply to determine if the secure link is alive,
- wherein sending the at least one ping message comprises sending the at least ping message *protected according to the security protocol*.

It is respectfully submitted that the Layer 2 test packet (L2TP Hello, L2F_ECHO, or PTP Echo-Request) as taught by Grosser *cannot be protected according to a security protocol*, as recited in claim 32.

Grosser focuses on testing a *Layer 2 tunnel* in a communications network. *See* Grosser 2:66-67 (“[T]he present invention provides a method and system for testing a Layer 2 tunnel.”). As expressly taught by Grosser, “the three Layer 2 tunnels discussed above do not themselves specify or provide data security.” Grosser, 4:23-24. In other words, the Layer 2 test packets sent in Layer 2 tunnels described in Grosser are *not* protected according to a security protocol.

As taught by the present application, the security protocol layer of a node is provided above the IP layer (*see* Fig. 2, layer 118 above the IP layer 116). The IP layer is at the Layer 3 level, which is above Layer 2 (the link layer). The Layer 2 test packets taught by Grosser are originated by a Layer 2 module in a node. For testing a Layer 2 tunnel, there is no reason for the Layer 2 test packets to be protected by the IPsec packet encryption mentioned in column 4, at lines 23-28 of Grosser. The column 4, lines 23-28, passage of Grosser refers to using PPP or IPsec packet encryption in conjunction with a Layer 2 VPN tunnel link to provide packet security between tunnel endpoints. This passage refers to protecting data packets that are sent through the IPsec layer. However, nowhere in Grosser is there any indication that the Layer 2 test packets are themselves protected by IPsec. Encrypting a lower level test packet, such as a Layer 2 test packet, using a higher level security protocol, such as IPsec, does not make much practical sense.

A higher layer data unit, such as an IPsec data unit, is *encapsulated* by a lower layer, such as layer 2. As is well known to persons of ordinary skill in the art, layer 3 information *passed down* to layer 2 (such as the data link layer) is treated as data and encapsulated with layer 2 header and trailer information. *See, e.g.*, “Introduction to Internet,” p. 7 (attached). Thus, a layer 2 packet contains the header, trailer, and data information of a layer 3 data unit. A higher layer data unit is always passed down to a lower layer. For a layer 2 test packet to be protected by IPsec, as suggested by the Office Action, the L2TP layer (layer 2) would have to be provided *above* the IPsec layer (layer 3), which is clearly prohibited.

The statement made by the Advisory Action that an L2TP packet is encapsulated in a UDP packet is erroneous. UDP (or TCP) is layer 4, which is two layers *higher* than layer 2. *See* “Introduction to Internet,” p. 6. For a layer 2 packet to be encapsulated in a UDP packet, layer 2 will have to be provided *above* layer 4, which is clearly erroneous.

It is therefore respectfully submitted that independent claim 32 is allowable over Grosser.

Independent claim 34, 36, and 38 are similarly allowable over Grosser.

Independent claim 5 has also been amended from dependent form to independent form with the scope of the claim remaining *unchanged*. Claim 5 recites that sending the at least one ping message comprises sending at least one Internet Control Message Protocol message. The Office Action conceded that Grosser fails to disclose sending an Internet control message protocol (ICMP) message as the ping message. 7/16/2004 Office Action at 9. However, the

Office Action relied upon Reid as teaching this missing element. It is respectfully submitted that a *prima facie* case of obviousness has not been established with respect to claim 5, for at least the reason that the Office Action has failed to establish that there was any motivation or suggestion to combine the teachings of Grosser and Reid. The Office Action has also failed to establish that there would be any reasonable expectation of success in combining Grosser and Reid, which is another requirement of the *prima facie* case of obviousness. See M.P.E.P. § 2143 (8th ed., Rev. 2), at 2100-129.

There simply did not exist any reason to incorporate the teachings of Reid regarding ICMP ping messages into the Layer 2 tunnel testing mechanism of Grosser. As discussed above, the focus of Grosser is on testing Layer 2 tunnels with *Layer 2* test packets. Using a higher level ping message in place of the Layer 2 test packets would *render the Grosser mechanism inoperative for its intended purpose*. It is respectfully submitted that an ICMP ping message, as taught by Reid, cannot be used to test a Layer 2 tunnel, which is the focus of the teachings of Grosser. “If [a] proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.” M.P.E.P. § 2143.01, at 2100-131. The Advisory Action stated that the “Grosser teachings are open ended in terms of a protocol used for a test packet (Col. 6 lines 30-60).” The cited column 6 passage of Grosser lists several alternative test messages for layer 2 – no suggestion is provided that a higher layer test message can be used.

The Office Action has failed to establish that there would have been a reasonable expectation of success in using the ICMP ping messages of Reid in testing Layer 2 tunnels of Grosser. See M.P.E.P. § 2143, at 2100-129 (“[T]here must be a reasonable expectation of success.”). It is highly unlikely that an ICMP message associated with a higher-level protocol can be used to successfully test a Layer 2 tunnel. More fundamentally, as Layer 2 test packets are available for testing Layer 2 tunnels, there would have been absolutely no reason whatsoever to employ a different level message, such as the ICMP ping message, to test the Layer 2 tunnels described in Grosser.

In view of the foregoing, it is respectfully submitted that a *prima facie* case of obviousness has not been established with respect to claim 5.

Claim 20 has also been amended from dependent form to independent form, with the scope of claim 20 remaining *unchanged*. Claim 20 is allowable over the asserted combination of Grosser and Reid for reasons similar to those given for claim 5.

In view of the foregoing, all claims are condition for allowance, which action is respectfully requested. The Commissioner is authorized to charge any additional fees and/or credit any overpayment to Deposit Account No. 20-1504 (NRB.0006US).

Respectfully submitted,

Date: _____

Nov 10, 2004



Dan C. Hu
Registration No. 40,025
TROP, PRUNER & HU, P.C.
8554 Katy Freeway, Suite 100
Houston, TX 77024
Telephone: (713) 468-8880
Facsimile: (713) 468-8883